

CLAIMS

What is claimed is:

- 1 1. A method for monitoring a database, comprising:
2 collecting user behavior data that indicates how one or more users use the database;
3 processing and storing the data as historical data;
4 analyzing the historical data to determine behavior patterns;
5 receiving a new set of data that indicates how one or more users have used the
6 database;
7 performing a comparison between the new set of data and the behavior pattern;
8 determining based on the comparison, whether the new set of data satisfies a set of
9 criteria;
10 if the new set of data satisfies the set of criteria, then determining that the new set of
11 data represents anomalous activity; and
12 responding to the determination by performing a targeted operation.
- 1 2. The method of claim 1, further comprising:
2 determining if the new set of data violates a rule based policy; and
3 if the new set of data violates the rule based policy, then determining that the new set
4 of data represents anomalous activity.
- 1 3. The method of claim 2, wherein collecting user behavior data further comprises:
2 reading information from an audit trail or dynamic performance views of the database
3 manager.

1 4. The method of claim 3, wherein collecting user behavior data further comprises
2 collecting information at a monitoring level selected from at least one of:
3 information about database access for one or more selected database objects;
4 information about database access for one or more selected database users; and
5 information about database access for one or more selected database user sessions.

1 5. The method of claim 3, wherein collecting user behavior data further comprises:
2 receiving a type of information to be monitored;
3 determining a monitoring level from the type of information; and
4 activating audit options of the database manager based upon the monitoring level
5 determined.

1 6. The method of claim 2, wherein analyzing the historical data to determine behavior
2 patterns further comprises:
3 determining a statistical model from the historical data.

1 7. The method of claim 6, wherein determining a statistical model from the historical
2 data further comprises:
3 determining a frequency of database access from the historical data;
4 determining a probability function for frequencies of database access; and
5 determining a cumulative probability function from the probability function.

1 8. The method of claim 7, wherein performing a comparison between the new set of
2 data and the behavior pattern further comprises:
3 testing a hypothesis using the new set of data against the statistical model.

1 9. The method of claim 8, wherein testing a hypothesis using the new set of data against
2 the statistical model further comprises:
3 determining a frequency of database access for the new set of data; and
4 determining the threshold value from a guard criteria and a probability function
5 parameter.

1 10. The method of claim 9, wherein testing a hypothesis using the new set of data against
2 the statistical model pattern further comprises:
3 comparing the frequency of database access for the new set of data with the threshold
4 value.

1 11. The method of claim 7, wherein the historical information is about database access
2 for one or more selected database objects and wherein determining a frequency of
3 database access from the historical data further comprises determining a frequency of
4 at least one of:
5 object access frequency by hour of day, object access frequency by hour of day and
6 operating system user, object access frequency by hour of day and database
7 user, object access frequency by hour of day and location, object access
8 frequency by hour of day and combination of at least two of operating system
9 user, database user and location.

1 12. The method of claim 7, wherein the historical information is about database access
2 for one or more selected database users and wherein determining a frequency of
3 database access from the historical data further comprises determining a frequency of
4 at least one of:
5 user access frequency by hour of day, user access frequency by hour of day and
6 operating system user, user access frequency by hour of day and database
7 user, user access frequency by hour of day and location, user access frequency
8 by hour of day and a combination of at least two of operating system user,
9 database user, and location.

1 13. The method of claim 7, wherein the historical information is about database access
2 for one or more selected database user sessions and wherein determining a frequency
3 of database access from the historical data further comprises determining a frequency
4 of at least one of:
5 number of page reads per session, access duration per session, number of page reads
6 per unit time.

1 14. The method of claim 1, wherein performing a targeted operation comprises at least
2 one of: raising an alert; sending an email; producing a report; performing a
3 visualization.

1 15. A computer-readable medium carrying one or more sequences of instructions for
2 reverting to a recovery configuration in response to device faults, which instructions,
3 when executed by one or more processors, cause the one or more processors to carry
4 out the steps of:
5 collecting user behavior data that indicates how one or more users use the database;
6 processing and storing the data as historical data;
7 analyzing the historical data to determine behavior patterns;
8 receiving a new set of data that indicates how one or more users have used the
9 database;
10 performing a comparison between the new set of data and the behavior pattern;
11 determining based on the comparison, whether the new set of data satisfies a set of
12 criteria;
13 if the new set of data satisfies the set of criteria, then determining that the new set of
14 data represents anomalous activity; and
15 responding to the determination by performing a targeted operation.

1 16. The computer-readable medium of claim 15, further comprising instructions which,
2 when executed by the one or more processors, cause the one or more processors to
3 carry out the steps of:
4 determining if the new set of data violates a rule based policy; and
5 if the new set of data violates the rule based policy, then determining that the new set
6 of data represents anomalous activity.

1 17. The computer-readable medium of claim 16, wherein the instructions for carrying out
2 the step of collecting user behavior data further comprise instructions for carrying out
3 the step of:
4 reading information from an audit trail of the database manager.

1 18. The computer-readable medium of claim 17, wherein the instructions for carrying out
2 the step of collecting user behavior data further comprise instructions for carrying out
3 the step of collecting information at a monitoring level selected from at least one of:
4 information about database access for one or more selected database objects;
5 information about database access for one or more selected database users; and
6 information about database access for one or more selected database user sessions.

1 19. The computer-readable medium of claim 17, wherein the instructions for carrying out
2 the step of collecting user behavior data further comprise instructions for carrying out
3 the steps of:
4 receiving a type of information to be monitored;
5 determining a monitoring level from the type of information; and
6 activating audit options of the database manager based upon the monitoring level
7 determined.

1 20. The computer-readable medium of claim 16, wherein the instructions for carrying out
2 the step of analyzing the historical data to determine behavior patterns further
3 comprise instructions for carrying out the step of:
4 determining a statistical model from the historical data.

1 21. The computer-readable medium of claim 20, wherein the instructions for carrying out
2 the step of determining a statistical model from the historical data further comprise
3 instructions for carrying out the step of:
4 determining a frequency of database access from the historical data;
5 determining a probability function for frequencies of database access; and
6 determining a cumulative probability function from the probability function.

1 22. The computer-readable medium of claim 21, wherein the instructions for carrying out
2 the step of performing a comparison between the new set of data and the behavior
3 pattern further comprise instructions for carrying out the step of:
testing a hypothesis using the new set of data against the statistical model.

1 23. The computer-readable medium of claim 22, wherein the instructions for carrying out
2 the step of testing a hypothesis using the new set of data against the statistical model
3 further comprise instructions for carrying out the steps of:
4 determining a frequency of database access for the new set of data; and
5 determining the threshold value from a guard criteria and a probability function
6 parameter.

1 24. The computer-readable medium of claim 23, wherein the instructions for carrying out
2 the step of testing a hypothesis using the new set of data against the statistical model
3 further comprise instructions for carrying out the step of:
4 comparing the frequency of database access for the new set of data with the threshold
5 value.

1 25. The computer-readable medium of claim 21, wherein the historical information is
2 about database access for one or more selected database objects and wherein the
3 instructions for carrying out the step of determining a frequency of database access
4 from the historical data further comprise instructions for carrying out the step of
5 determining a frequency of at least one of:
6 object access frequency by hour of day, object access frequency by hour of day and
7 operating system user, object access frequency by hour of day and database
8 user, object access frequency by hour of day and location and object access
9 frequency by hour of day and a combination of at least two of operating
10 system user, database user and location.

1 26. The computer readable medium of claim 21, wherein the historical information is
2 about database access for one or more selected database users and wherein the
3 instructions for carrying out the step of determining a frequency of database access
4 from the historical data further comprise instructions for carrying out the step of
5 determining a frequency of at least one of:
6 user access frequency by hour of day, user access frequency by hour of day and
7 operating system user, user access frequency by hour of day and database

8 user, user access frequency by hour of day and location and user access
9 frequency by hour of day and a combination of at least two of operating
10 system user, database user, and location.

1 27. The computer readable medium of claim 21, wherein the historical information is
2 about database access for one or more selected database user sessions and wherein the
3 instructions for carrying out the step of determining a frequency of database access
4 from the historical data further comprise instructions for carrying out the step of
5 determining a frequency of at least one of:
6 number of page reads per session, access duration per session, number of page reads
7 per unit time.

1 28. The computer readable medium of claim 15, wherein the instructions for carrying out
2 the step of performing a targeted operation comprises instructions for
3 carrying out at least one of: raising an alert; sending an email; producing a report;
4 performing a visualization.

1 29. An apparatus, comprising:
2 means for collecting user behavior data that indicates how one or more users use the
3 database;
4 means for processing and storing the data as historical data;
5 means for analyzing the historical data to determine behavior patterns;
6 means for receiving a new set of data that indicates how one or more users have used
7 the database;

8 means for performing a comparison between the new set of data and the behavior
9 pattern;
10 means for determining based on the comparison, whether the new set of data satisfies
11 a set of criteria;
12 means for determining that the new set of data represents anomalous activity, if the
13 new set of data satisfies the set of criteria; and
14 means for responding to the determination by performing a targeted operation.

1 30. An apparatus, comprising:
2 a data collector for collecting user behavior data that indicates how one or more users
3 use the database and processing and storing the data as historical data; and
4 receiving a new set of data that indicates how one or more users have used the
5 database;
6 a data analyzer for analyzing the historical data to determine behavior patterns; and
7 an anomaly detector for performing a comparison between the new set of data and the
8 behavior pattern; determining based on the comparison, whether the new set
9 of data satisfies a set of criteria; determining that the new set of data
10 represents anomalous activity if the new set of data satisfies the set of criteria;
11 and responding to the determination by performing a targeted operation.